UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JOSEPH HALEY, ROWDY ALLDRIDGE, and MARY LEA KIRBY, individually on behalf of themselves and all others similarly situated, Plaintiffs, - against - INTERNATIONAL BUSINESS MACHINES CORPORATION and JOHNSON & JOHNSON HEALTH CARE SYSTEMS, INC., Defendant.	Civil Action No. **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Joseph Haley, Rowdy Alldridge, and Mary Lea Kirby (collectively "Plaintiffs") by and through their attorneys of record, upon personal knowledge as to their own acts and experiences, and upon information and belief as to all other matters, bring this class action complaint on behalf of themselves and a class as defined below ("Class"), against defendants International Business Machines Corporation and Johnson & Johnson Health Care Systems, Inc. (collectively "Defendants"), and allege as follows:

INTRODUCTION

1. Plaintiffs bring this class action against Defendants for their failure to properly manage, maintain, secure and/or safeguard Plaintiffs and Class members' protected medical and health information stored within information networks and servers for which they are responsible, including, without limitation, Plaintiffs and Class members' "protected health information" (PHI)[1] and "personally identifiable information" (PII),[2] (collectively, PHI and PII are also referred to herein as "Private Information").

2. Each of the Defendants managed, acquired, collected, and stored Plaintiffs and Class members' PII and PHI to facilitate the healthcare-related services Plaintiffs and Class members requested or received. Each Defendant knew, at all times material, that they were managing, collecting, storing, and/or responsible for the security of sensitive data, including Plaintiffs and Class members' highly confidential PII and PHI.

---

[1] PHI is a category of information that refers to an individual's medical records and history, which is protected under the Health Insurance Portability and Accountability Act. Inter alia, PHI includes test results, procedure descriptions, diagnoses, personal or family medical histories, and data points applied to a set of demographic information for a particular patient. PHI is inclusive of and incorporates personally identifiable information.

[2] PII generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on its face name an individual, but that are considered to be particularly sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport numbers, driver's license numbers, financial account numbers).

3. Plaintiffs seek to hold Defendants responsible for the harms they caused and will continue to cause Plaintiffs and the members of the Class arising from a preventable cyberattack occurring no later than August 2, 2023, by which cyber criminals infiltrated the database that supports Janssen Carepath, a Johnson & Johnson Health Care Systems Inc. entity. Defendants' inadequately managed, maintained, and/or protected the network in which highly sensitive PHI/PII was being kept unprotected ("Data Breach").

4. Although the Data Breach occurred no later than August 2, 2023, if not sooner, Defendants did not inform Plaintiffs and victims of the Data Breach – members of the Class – until no earlier than September 29, 2023 and thereafter, thereby leaving them wholly unaware of said breach and consequently keeping them vulnerable to the misuse of their PHI and PII as a consequence of the cyberattack.

5. Defendants failed to ensure that Plaintiffs and the Class members' Private Information was managed and maintained in a manner consistent with standards established in the industry, standards and duties imposed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule ("45 CFR, Part 160 and Parts A and E of Part 164"), the HIPAA Security Rule ("45 CFR, Part 160 and Subparts A and C of Part 164") and other relevant standards.

6. State and federal statutes and regulations, as well as common law principles impose a duty on Defendants to maintain the confidentiality of such information.

7. For example, HIPAA establishes obligations for the protection of individuals' medical records and other personal health information. HIPAA, in general, applies to healthcare providers, health plans/insurers, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically, and sets requirements for Defendants' maintenance of Plaintiffs and Class members' health care related PII and PHI. More specifically, HIPAA requires appropriate safeguards be maintained by organizations such as Defendants to protect the privacy of patient health information and sets limits and conditions on the uses and disclosures that may be made of such information without express customer/patient authorization.

8. Additionally, the so-called "HIPAA Security Rule" establishes national standards to protect individuals' electronic health information that is created, received, used, or maintained by a covered entity. The HIPAA Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.

9. By obtaining, collecting, storing, using, and/or managing Plaintiffs and Class members' PII and PHI, Defendants assumed legal and equitable duties to those individuals, including the duties that arise from HIPAA and other state and federal statutes and regulations, as well as common law principles.

10. Defendants disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiffs and Class members' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII and PHI of Plaintiffs and Class members was compromised and damaged through access by and disclosure to an unknown and unauthorized third party – an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class members in the future – and Plaintiffs and Class members are entitled to damages. In addition, Plaintiff and Class members, who have a continuing interest in ensuring that their information is and remains safe, are entitled to injunctive and other equitable relief.

PARTIES

Plaintiffs

11. Plaintiff Joseph Haley is, and at all relevant times was, a resident of Hernando and a citizen of the state of Mississippi. In early October 2023, Plaintiff Haley received a notice, dated September 29, 2023, from IBM stating that "personal information contained within a database used on the Janssen Carepath platform" had been accessed in the Data Breach. The Notice stated that the following information was included in the Data Breach: "contact information, health insurance information, and information about medications and associated conditions that were

provided to the Janssen Carepath application." Plaintiff Haley is deeply concerned about protecting his personal health information from public disclosure. Plaintiff Haley maintains credit monitoring services through Experian. Since August 2023, Mr. Haley has received numerous notices from Experian indicating that his personal information is on the dark web. In addition, since August 2023, Plaintiff Haley has experienced a dramatic increase in the number of spam phone calls he receives every day. Many of these recently received spam calls claim to be offering healthcare related services.

12. Plaintiff Rowdy Alldridge is, and at all relevant times was, a resident of Idaho Falls and a citizen of the state of Idaho. In early October 2023, Plaintiff Alldridge received a notice, dated September 29, 2023, from IBM stating that "personal information contained within a database used on the Janssen Carepath platform" had been accessed in the Data Breach. The Notice stated that the following information was included in the Data Breach: "contact information, health insurance information, and information about mediations and associated conditions that were provided to the Janssen Carepath application." Plaintiff Alldridge is deeply concerned about protecting his personal health information from public disclosure.

13. Plaintiff Mary Lea Kirby is, and at all relevant times was, a resident of Brunswick and a citizen of the state of Ohio. In early October 2023, Plaintiff Kirby received a notice, dated September 29, 2023, from IBM stating that "personal information contained within a database used on the Janssen Carepath platform" had been accessed in the Data Breach. The Notice stated that the following information was included in the Data Breach: "contact information, health insurance information, and information about mediations and associated conditions that were provided to the Janssen Carepath application." Plaintiff Kirby is deeply concerned about protecting his personal health information from public disclosure.

Defendants

14. Defendant International Business Machines Corporation ("IBM") is a New York corporation with its principal place of business located at One Orchard Road, Armonk, NY 10504.

Defendant IBM provides "infrastructure, software, and consulting services for clients as they pursue the digital transformation of the world's mission-critical businesses." IBM is a service provider to health care entity Johnson & Johnson Health Care Systems, which relied on IBM to manage the application and database that supports Janssen Carepath.

15. Defendant Johnson & Johnson Health Care Systems, Inc. is a New Jersey corporation with a principal place of business located at 425 Hoes Lane, Piscataway, NJ 08854. Defendant Johnson & Johnson Health Care Systems Inc., owns Janssen Carepath and provides contracting, supply chain, and health care related business support services ("J&J").

16. Defendants IBM and J&J managed, maintained, collected and/or stored the PII and PHI of Plaintiffs and Class members in the ordinary course of their businesses.

JURISDICTION AND VENUE

17. This Court has subject matter jurisdiction over this case pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, which affords federal courts with original jurisdiction over cases where any member of the plaintiff class is a citizen of a state different from any defendant, and where the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Here, the Nationwide Class, as defined below, includes recipients of Defendants' Notice of Data Breach, discussed herein, which, upon information and belief, include non-New York or New Jersey citizens. Since Defendant IBM is headquartered in New York, and Defendant J&J is headquartered in New Jersey, there is minimal diversity between at least one member of the Plaintiffs' nationwide class and Defendants.

18. This Court has general personal jurisdiction over Defendant IBM because it operates its principal place of business in the District. Additionally, this Court also has specific personal jurisdiction over the Defendants because they each have minimum contacts with the District, as they conduct substantial business in or from the District.

19. This Court has supplemental jurisdiction over any claims not arising, in whole or in part, from violation of federal law.

20. This Court is the proper venue for this action pursuant to 28 U.S.C. § 1391(a) and (b) because a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this District, and because Defendants conduct a substantial part of their business within this District.

FACTUAL BACKGROUND

The Data Breach

21. On or about September 29, 2023, Defendant IBM sent Plaintiffs and other victims of the Data Breach a Notice of Data Breach ("Notice Letter"), informing them of an "incident involving unauthorized access to personal information contained within a database used on the Janssen Carepath platform, a patient support platform that offers savings options and other patient support resources."

22. The Notice Letter, an exemplar of which is attached hereto as Exhibit A, acknowledges that Defendant IBM's investigation identified on August 2, 2023 there was an unauthorized access to personal information on the database, but was unable to determine its scope. The IBM Notice Letter acknowledged that the "personal information involved in the incident may have included your name and one or more of the following: contact information, health insurance information, and information about mediations, and associated conditions that were provided to Janssen Carepath." In other words, PHI and PII was accessed in the Data Breach. While IBM currently maintains that Social Security numbers were not contained in the database or affected, Plaintiffs reserve the right to contend that they were also accessed after a reasonable opportunity for discovery.

23. To date, Defendants have failed to disclose the actual root cause of the Data Breach, the vulnerabilities exploited, and why it took until September 29, 2023 to inform Plaintiffs, each of whom has a vested interest in ensuring that their Private Information remains protected.

24. This "disclosure" amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiffs and Class members of the Data Breach's critical facts. Without

these details, Plaintiffs and Class members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

25. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were managing, collecting, storing or maintaining for Plaintiffs and Class members, ultimately causing the exposure of their Private Information.

26. Upon information and belief, Defendants continue to manage, collect, store, or maintain Plaintiffs' PHI and PII, as well as that of all other Class members.

Defendants' Business and Obligation to Preserve and Protect Confidentiality and Privacy

27. As a consequence of securing or receiving services from Janssen Carepath, Plaintiffs and Class members provided sensitive and confidential Private Information, including their names and Social Security Numbers, and other sensitive information.

28. Plaintiffs and Class members provided their Private Information with the reasonable expectation and mutual understanding that Janssen Carepath – and related entities and their service providers, such as the Defendants – would comply with their obligations to keep such information confidential and secure from unauthorized access.

29. Plaintiffs and Class members relied on the sophistication of Defendants to keep their Private Information confidential and securely managed and maintained, to only permit the use of this information for necessary purposes, and to make only authorized disclosures of this information. Plaintiffs and Class members, who value the confidentiality of their Private Information and demand security to safeguard their Private Information, took reasonable steps to maintain the confidentiality of their PII/PHI.

30. At all times material, Defendants were under a duty to adopt and implement reasonable measures to protect the Private Information of Plaintiffs and Class members from involuntary disclosure to third parties. Defendants also have legal duties created by The Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act"), HIPAA, their contract with Plaintiffs and Class members, industry standards, and their representations made to Plaintiffs and Class

members, to keep Plaintiffs and Class members' Private Information confidential and to protect it from unauthorized access and disclosure.

31. By obtaining, collecting, using, storing, and/or managing Plaintiffs and Class members' Private Information, Defendants assumed legal and equitable duties, and knew or should have known that they were responsible for protecting Plaintiffs and Class members' Private Information from unauthorized disclosure.

32. Defendants' negligence in safeguarding the Private Information of Plaintiffs and Class members is exacerbated by Defendants' repeated warnings and alerts informing Plaintiffs and Class members that their Private Information was protected and secure.

33. Defendants' HIPAA Policy relating to the confidentiality of PHI clearly states:

> . . . we are required by law to maintain the privacy of "protected health information." "Protected health information" includes any individually identifiable information that we obtain from you or others that relate to your past, present or future physical or mental health, the health care you have received, or payment for your health care.
>
> As required by law, this notice provides you with information about your rights and our legal duties and privacy practices with respect to the privacy of protected health information. This notice also discusses the uses and disclosures we will make of your protected health information. We must comply with the provisions of this notice as currently in effect, although we reserve the right to change the terms of this notice from time to time and to make the revised notice effective for all protected health information we maintain.

34. Defendants had obligations created by HIPAA, contract, industry standards, common law, and their own promises and representations made to Plaintiffs and Class members to keep their Private Information confidential and protect it from unauthorized access and disclosure.

35. Plaintiffs and Class members had a reasonable expectation and mutual understanding that Defendants would comply with their obligations to keep the Private Information they collected confidential and secure from unauthorized access and disclosure.

36. Defendants failed to use reasonable security procedures and practices appropriate to safeguard the sensitive, unencrypted information it was maintaining for Plaintiffs and Class

members, consequently enabling and causing the exposure of Private Information of hundreds of thousands of individuals.

37. Because of Defendants' negligence and misconduct in failing to keep information confidential, the unencrypted Private Information of Plaintiffs and Class members has been expropriated by unauthorized individuals who can now access the PHI and PII of Plaintiffs and Class members and use it as they please.

38. Plaintiffs and Class members now face a real, present and substantially increased risk of fraud and identity theft and have lost the benefit of the bargain they made with Defendants when receiving services.

Data Breaches Lead to Identity Theft and Cognizable Injuries.

39. The PII and PHI of consumers, such as Plaintiffs and Class members, is valuable and has been commoditized in recent years.

40. Defendants were also aware of the significant repercussions that would result from their failure to protect Plaintiffs and Class members' Private Information and knew, or should have known, the importance of safeguarding the Private Information collected, stored, or managed by or entrusted to them and of the foreseeable consequences if Defendants' data security was breached. Nonetheless, Defendants failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

41. Identity theft associated with data breaches is particularly pernicious due to the fact that the information is made available, and has usefulness to identity thieves, for an extended period of time after it is stolen. As a result, victims suffer both immediate and long-lasting exposure and are susceptible to further injury over the passage of time.

42. As a direct and proximate result of Defendants' conduct, Plaintiffs and the other Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. They must now be vigilant and continuously review their credit reports for suspected incidents of identity theft, educate themselves about security freezes, fraud

alerts, and take steps to protect themselves against identity theft, which will extend indefinitely into the future.

43. Even absent any adverse use, consumers suffer injury from the simple fact that information associated with their financial and health care accounts and identity has been stolen. When such sensitive information is stolen, accounts become less secure. Information once used to sign up for bank accounts and other financial services is no longer as reliable as it had been before the theft. Thus, consumers must spend time and money to re-secure their financial position and rebuild the good standing they once had in the financial community.

44. Plaintiffs and the other Class members also suffer ascertainable losses in the form of opportunity costs and the time and costs reasonably incurred to remedy or mitigate the effects of the Data Breach, including:

A. Monitoring compromised accounts for fraudulent charges;

B. Canceling and reissuing credit and debit cards linked to the financial information in possession of Defendants;

C. Purchasing credit monitoring and identity theft prevention;

D. Addressing their inability to withdraw funds linked to compromised accounts;

E. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

F. Taking trips to banks and waiting in line to verify their identities in order to restore access to the accounts;

G. Placing freezes and alerts with credit reporting agencies;

H. Spending time on the phone with or at financial institutions to dispute fraudulent charges;

I. Contacting their financial institutions and closing or modifying financial accounts;

J. Resetting automatic billing and payment instructions from compromised credit and debit cards to new cards;

K. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised accounts that had to be cancelled;

L. Closely reviewing and monitoring financial accounts and credit reports for unauthorized activity for years to come; and

M. Taking measures to protect themselves from incidents of identity theft by nefarious actors who have unlawfully obtained intimate personal details and information respecting their health, medical condition and other confidential personal matters.

45. Moreover, Plaintiffs and the other Class members have an interest in ensuring that Defendants implement reasonable security measures and safeguards to maintain the integrity and confidentiality of the Private Information, including making sure that the storage of data or documents containing Private Information is not accessible to unauthorized persons, that access to such data is sufficiently protected, and that the Private Information remaining in the possession of Defendants is fully secure, remains secure, and is not subject to future theft.

46. As a further direct and proximate result of Defendants' actions and inactions, Plaintiffs and the other Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

47. As a direct and proximate result of Defendants' wrongful actions or omissions here, resulting in the Data Breach and the unauthorized release and disclosure of Plaintiffs and other Class members' Private Information, Plaintiffs and Class members have suffered, and will continue to suffer, ascertainable losses, economic damages, and other actual injury and harm, including, *inter alia*, (i) the resulting increased and imminent risk of future ascertainable losses, economic damages and other actual injury and harm, (ii) the opportunity cost and value of lost time they must spend to monitor their financial accounts and other accounts—for which they are

entitled to compensation; and (iii) emotional distress as a result of having their Private Information accessed and exfiltrated in the Data Breach.

Defendants Were Well Aware of the Threat of Cyber Theft and Exfiltration in the Healthcare Industry

48. Plaintiffs and Class members entrust healthcare providers, related service providers, and related entities with highly sensitive and confidential Private Information. Defendants, in turn, collected, stored, and/or maintained that information and agreed to protect that PHI and PII pursuant to HIPAA and to prevent its disclosure.

49. Plaintiffs and Class members were required to provide their Private Information with the reasonable expectation and mutual understanding that Janssen Carepath and entities such as the Defendants would comply with their obligations to keep such information confidential and secure from unauthorized access and disclosure.

50. Defendants could have prevented the Data Breach by assuring that the Private Information at issue was properly secured.

51. Defendants' overt negligence in safeguarding Plaintiffs and Class members' PII and PHI is exacerbated by repeated warnings and alerts directed to protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent years. Further, as entities in or managing Private Information secured by or within the healthcare space, Defendants were on notice that companies directly providing healthcare and related services operating in the healthcare industry, are targets for data breaches.

52. The healthcare industry in particular has experienced a large number of high-profile cyberattacks. Cyberattacks, generally, have become increasingly more common. In 2021, a record 715 healthcare data breaches reported, an increase of approximately 100% since 2017.[3]

[3] 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/2022-healthcare-data-breach-report/ (last accessed October 31, 2023).

53. This trend continued in 2022, with 707 healthcare breaches reported, still near record highs.[4] Additionally, according to the HIPAA Journal, the five largest healthcare data breaches reported in 2022 impacted the healthcare records of approximately 13.3 million people.[5] Thus, Defendants were on further notice regarding the increased risks of inadequate cybersecurity. In February 2022, the cybersecurity arm of the U.S. Department of Health and Human Services ("HHS") issued a warning to hospitals and healthcare systems about a dramatic rise in cyberattacks, including ransomware attacks, urging facilities to shore up their cyber defenses.[6] Indeed, HHS's cybersecurity arm has issued yet another warning about increased cyberattacks that urged vigilance with respect to data security.[7]

54. In the context of data breaches, healthcare is "by far the most affected industry sector."[8] Further, cybersecurity breaches in the healthcare industry are particularly devastating,

[4] *Id*.

[5] *Id*.

[6] Rebecca Pifer, Tenet says 'cybersecurity incident' disrupted hospital operations, HEALTHCAREDIVE (Apr. 26, 2022), https://www.healthcaredive.com/news/tenet-sayscybersecurity-incident-disrupted-hospital-operations/622692/ (last accessed October 31, 2023).

[7] *Id*. (HHS warned healthcare providers about the increased potential for attacks by a ransomware group called Hive, "[c]alling it one of the 'most active ransomware operators in the cybercriminal ecosystem,' the agency said reports have linked Hive to attacks on 355 companies within 100 days of its launch last June — nearly three a day.").

[8] Tenable Security Response Team, *Healthcare Security*, TENABLE (Mar. 10, 2021), https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches (last accessed October 31, 2023).

given the frequency of such breaches and the fact that healthcare providers maintain highly sensitive and detailed PII.[9]

55. A TENABLE study analyzing publicly disclosed healthcare sector breaches from January 2020 to February 2021 reported that "records were confirmed to have been exposed in nearly 93% of the breaches."[10]

56. This is such a breach of cybersecurity where highly detailed PII and PHI records maintained and collected by a healthcare entity were accessed and/or acquired by a cybercriminal.

57. Due to the high-profile nature of these breaches, and other breaches of its kind, Defendants were and/or certainly should have been on notice and aware of such attacks occurring in the healthcare industry and, therefore, should have assumed and adequately performed the duty of preparing for such an imminent attack. This is especially true given that Defendants are large, sophisticated operations with the resources to put adequate data security protocols in place and assure the security of the data collected by them and entrusted to them by Plaintiff and Class members.

58. Yet, despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect Plaintiffs and Class members' PII and PHI from being compromised.

Defendants' Conduct Violates Federal Law, Including the Rules and Regulations of HIPAA and HITECH

59. Entities providing health care services or managing health care related data, have a statutory duty under HIPAA and other federal or state statutes to safeguard Plaintiffs and Class members' data.

60. Moreover, Plaintiffs and Class members surrendered their highly sensitive personal data under the implied condition and their reasonable expectation and belief that Defendants would

[9] *Id.*

[10] *Id.*

keep it private and secure. Accordingly, Defendants also have an implied duty to safeguard their data, independent of any statute.

61. Title II of HIPAA contains so-called Administrative Simplification provisions, 42 U.S.C. §§ 1301, *et seq.*, requiring, among other things, that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI like the data Defendants left unguarded. The HHS subsequently promulgated multiple regulations, which include 45 C.F.R. § 164.306(a)(1-4); 45 C.F.R. § 164.312(a)(1); 45 C.F.R. § 164.308(a)(1)(i); 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

62. Defendants, by reason of their roles, are covered entities pursuant to HIPAA. *See* 45 C.F.R. § 160.102. Defendants must therefore comply with the HIPAA Privacy Rule and Security Rule. See 45 C.F.R. Part 160 and Part 164, Subparts A through E.

63. Defendants, by reason of their roles, are also covered entities pursuant to the Health Information Technology Act ("HITECH").[11] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

64. Because Defendants are covered by HIPAA, they are required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

65. HIPAA's Privacy Rule or Standards for Privacy of Individually Identifiable Health Information establishes national standards for the protection of health information.

66. HIPAA's Privacy Rule or Security Standards for the Protection of Electronic Protected Health Information establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

[11] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

67. HIPAA requires covered entities to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

68. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

69. HIPAA's Security Rule requires covered entities to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits; protect against any reasonably anticipated threats or hazards to the security or integrity of such information; protect Against reasonably anticipated uses or disclosures of such information that are not permitted; and ensure compliance by their workforce.

70. HIPAA also requires covered entities to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information" under 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

71. Moreover, the HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, requires covered entities to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

72. Plaintiffs and Class members' personal and medical information, including their PII and PHI, is "protected health information" as defined by 45 CFR § 160.103.

73. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

74. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

75. Plaintiffs and Class members' personal and medical information, including their PII and PHI, is "unsecured protected health information" as defined by 45 CFR § 164.402.

76. Plaintiffs and Class members' unsecured protected health information has been acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

77. Plaintiffs and Class members' unsecured protected health information acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

78. Plaintiffs and Class members' unsecured protected health information that was acquired, accessed, used, or disclosed in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

79. Plaintiffs and Class members' unsecured protected health information was viewed by unauthorized persons in a manner not permitted under 45 CFR Subpart E as a result of the Data Breach.

80. After receiving notice that they were victims of a data breach that required the filing of a Breach Report in accordance with 45 CFR § 164.408(a), it is reasonable for recipients of that notice, including Plaintiff and Class members in this case, to believe that future harm (including identity theft) is real and imminent, and to take steps to mitigate that risk of future harm.

81. HIPAA requires covered entities to protect against reasonably anticipated threats to the security of sensitive patient health information.

82. Covered entities must implement safeguards to ensure the confidentiality, integrity, and availability of PHI. Safeguards must include physical, technical, and administrative components.

83. This Data Breach is considered a breach under the HIPAA Rules because there is an access of PHI not permitted under the HIPAA Privacy Rule:

> A breach under the HIPAA Rules is defined as, "the acquisition, access, use, or disclosure of PHI in a manner not permitted under the [HIPAA Privacy Rule] which compromises the security or privacy of the PHI." See 45 C.F.R. 164.40.

84. The Data Breach could have been prevented if Defendants had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored their obligations to their patients.

85. Defendants' security failures include, but are not limited to: failing to maintain an adequate data security system and safeguards to prevent data loss; failing to mitigate the risks of a data breach and loss of data, including identifying internal and external risks of a security breach; failing to ensure the confidentiality and integrity of electronic protected health information that Defendants create, receive, maintain, and transmit in violation of 45 CFR 164.306(a)(1); failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1); failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1); failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information in violation of 45 CFR 164.306(a)(2); failing to protect against any reasonably-anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 CFR 164.306(a)(3); impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons in violation of 45 CFR 164.502, *et seq.*; and retaining information past a recognized purpose and not deleting it.

86. Upon information and belief, prior to the Breach, Defendants were aware of their security failures but failed to correct them or to disclose them to the public, including Plaintiffs and Class members.

87. The implementation of proper data security processes requires affirmative acts. Accordingly, Defendants knew or should have known that they did not take such actions and failed to implement adequate data security practices.

88. Because Defendants have failed to comply with industry standards, while monetary relief may cure some of Plaintiffs and Class members' injuries, injunctive relief is necessary to ensure Defendants' approach to information security is adequate and appropriate. Defendants still manage, collect, store, or maintain the PII and PHI of Plaintiff and Class members; and without the supervision of the Court via injunctive relief, Plaintiffs and Class members' PII and PHI remains at risk to subsequent Data Breaches.

89. In addition to their obligations under federal and state laws, Defendants owed a duty to the Plaintiffs and Class members to exercise reasonable care in managing, obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendants owed a duty to Plaintiffs and Class members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that their computer systems, networks, and protocols adequately protected the Private Information of Plaintiffs and Class members.

90. Defendants further owe a duty to Plaintiffs and Class members to mitigate the harm suffered by Plaintiffs' and Class members as a result of the Data Breach.

FTC Guidelines Prohibiting Unfair or Deceptive Acts

91. The FTC Act restricts companies from engaging in "unfair or deceptive acts or practices in or affecting commerce." The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an

"unfair practice" in violation of the FTC Act. *See e.g., FTC v. Wyndham Corp.*, 799 F.3d 236 (3d Cir. 2015).

92. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[12]

93. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[13]

94. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

95. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

96. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act.

---

[12] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited October 31, 2023).

[13] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last visited October 31, 2023.

97. Defendants were at all times fully aware of their obligations to protect Plaintiffs and Class members' Private Information because of their business model of collecting Private Information and storing such information. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Value of the Relevant Sensitive Information

98. Electronic health records contain a plethora of sensitive information (e.g., patient data, patient diagnosis, lab results, RX's, treatment plans) that is valuable to cyber criminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PII and PHI and financial information are valuable commodities for which a "cyber black market" exists in which criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on a number of underground internet websites. Unsurprisingly, the healthcare industry is at high risk for and acutely affected by cyberattacks.

99. The high value of PII and PHI and financial information to criminals is further evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[14] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. *Id.* Criminals can also purchase access to entire company data breaches from $999 to $4,995.[15]

---

[14] Your personal data is for sale on the dark web. Here's how much it costs, Digital Trends, Oct. 16, 2019, available at: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it costs/#:~:text=To%20gain%20access%20to%20someone%27s,range%20of%20%2450%20to%20%24200. (last visited October 31, 2023).

[15] In the Dark, VPNOverview, 2019, available at: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ last visited October 31, 2023.

100. Between 2005 and 2019, at least 249 million people were affected by health care data breaches.[16] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[17] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03% of overall health data breaches, according to cybersecurity firm Tenable.[18]

101. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members. For example, it is believed that certain PII compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud will be an omnipresent threat for Plaintiff and Class members for the rest of their lives. They will need to remain constantly vigilant.

102. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."

103. Identity thieves can use PII and PHI and financial information, such as that of Plaintiffs and Class members, which Defendants failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various types of government fraud such as immigration fraud, obtaining a driver's license or identification card in the victim's

[16] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133 last visited October 31, 2023.

[17] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ last visited October 31, 2023.

[18] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches last visited October 31, 2023.

name but with another's picture, using the victim's information to obtain government benefits, or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

104. The ramifications of Defendants' failure to keep secure Plaintiffs and Class members' PII and PHI are long lasting and severe. Once PII and PHI and financial information is stolen, particularly identification numbers, fraudulent use of that information and damage to victims may continue for years. Indeed, the PII and PHI of Plaintiffs and Class members was taken by hackers to engage in identity theft or to sell it to other criminals who will purchase the PII and PHI for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

105. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII and PHI and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

106. The harm to Plaintiffs and Class members is especially acute given the nature of the leaked data. Medical identity theft is one of the most common, most expensive, and most difficult-to-prevent forms of identity theft. According to Kaiser Health News, "medical- related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013,"

[19] 47 Report to Congressional Requesters, GAO, at 29 (June 2007), available at: http://www.gao.gov/new.items/d07737.pdf last visited October 31, 2023.

which is more than identity thefts involving banking and finance, the government and the military, or education.[20]

107. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[21]

108. If cyber criminals manage to access financial information, health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Defendants may have exposed Plaintiffs and Class members.

109. A study by Experian found that the average total cost of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[22] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third saw their insurance premiums rise, and forty percent were never able to resolve their identity theft at all.[23]

---

[20] Michael Ollove, The Rise of Medical Identity Theft in Healthcare, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/ last visited October 31, 2023.

[21] *Id.*

[22] See Elinor Mills, Study: Medical Identity Theft is Costly for Victims, CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ last visited October 31, 2023.

[23] *Id.*; *see also* Healthcare Data Breach: What to Know About them and What to Do After One, EXPERIAN, available at https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ last visited October 31, 2023.

110. Data breaches are preventable.[24] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[25] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised."[26]

111. Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures…. Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[27]

112. The Data Breach resulted from a combination of insufficiencies that demonstrate Defendants failed to comply with safeguards and concomitant duties mandated and required by HIPAA regulations.

Defendants' Delayed Response to the Breach

113. Time is of the essence when highly sensitive PII and PHI is subject to unauthorized access and/or acquisition. The disclosed, accessed, and/or acquired PII and PHI of Plaintiffs and Class members is likely available on the Dark Web. Hackers can access and then offer for sale the unencrypted, unredacted PII and PHI to criminals. Plaintiffs and Class members are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from the possible publication of their PII and PHI, especially their Social Security numbers and sensitive medical information, onto the Dark Web. Plaintiffs and Class members now face a lifetime risk of identity

---

[24] Lucy L. Thompson, Despite the Alarming Trends, Data Breaches Are Preventable, in DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

[25] *Id.* at 17.

[26] *Id*. at 28.

[27] *Id.*

theft, which is heightened here by unauthorized access, disclosure, and/or activity by cybercriminals on computer systems containing hundreds of thousands of Medicare numbers, Social Security numbers, Dates of birth, and other critical PHI and/or PII.

114. Despite this understanding, Defendants delayed informing affected individuals, including Plaintiff and Class members, about the Data Breach. And the Notice Letter provided only scant details of the Data Breach and Defendants' recommended next steps.

115. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.8% of U.S.-based workers are compensated on an hourly basis, while the other 44.2% are salaried.[28]

116. According to the U.S. Bureau of Labor Statistics' 2018 American Time Use Survey, American adults have only 36 to 40 hours of "leisure time" outside of work per week;[29] leisure time is defined as time not occupied with work or chores and is "the time equivalent of 'disposable income.'"[30] Usually, this time can be spent at the option and choice of the consumer, however, having been notified of the Data Breach, consumers now have to spend hours of their leisure time self-monitoring their accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

117. Plaintiffs and Class members are now deprived of the choice as to how to spend their valuable free hours and seek remuneration for the loss of valuable time as another element of damages.

---

[28] U.S. BUREAU OF LABOR STATISTICS, Characteristics of minimum wage workers, 2021, available at https://www.bls.gov/opub/reports/minimum-wage/2021/pdf/home.pdf, last visited October 31, 2023; *see also*, Bureau of Labor Statistics, https://www.bls.gov/news.release/empsit.t19.htm, last visited June 19, 2023 (finding that on average, private-sector workers make $1,146.99 per 40-hour work week).

[29] See https://www.cnbc.com/2019/11/06/how-successful-people-spend-leisure-time-james-wallman.html last visited October 31, 2023.

[30] *Id.*

I. CLASS ALLEGATIONS

118. Pursuant to Fed. R. Civ. P. 23(b)(1), (b)(2), (b)(3), and (c)(4), Plaintiffs assert common law claims, as more fully alleged hereinafter, on behalf of the following Nationwide Class:

> **Nationwide Class**: All residents of the United States whose PII or PHI was accessed or otherwise compromised as a result of the Data Breach.

Members of the Nationwide Class are also referred to herein collectively as "Class members" or "Class."

119. Excluded from the Class are Defendants, any entity in which Defendants have a controlling interest, and Defendants' officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

120. The proposed Class meets the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

121. **Numerosity**: The exact number of members of the Class is unknown to Plaintiffs at this time. Defendants provide services to millions of consumers. The Data Breach victimized hundreds of thousands of members of the Class, making joinder of each individual impracticable. Ultimately, members of the Class will be readily identified through Defendants' records.

122. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a) Whether Defendants failed to adequately safeguard Plaintiffs' and the Class members' PII and PHI;

b) Whether Defendants failed to protect Plaintiffs' and the Class members' PII and PHI, as promised;

c) Whether Defendants' computer system systems and data security practices

used to protect Plaintiffs' and the Class members' PII and PHI violated HIPAA, federal, state and local laws, or Defendants' duties;

d) Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiffs' and the Class members' PII and PHI properly and/or as promised;

e) Whether Defendants violated the consumer protection statutes, data breach notification statutes, state unfair practice statutes, state privacy statutes, and state medical privacy statutes, HIPAA, and/or FTC law or regulations, imposing duties upon Defendants, applicable to Plaintiffs and Class members;

f) Whether Defendants failed to notify Plaintiffs and members of the Class about the Data Breach as soon as practical and without delay after the Data Breach was discovered;

g) Whether Defendants acted negligently in failing to safeguard Plaintiffs' and the Class members' PII and PHI;

h) Whether Plaintiffs and the Class members are entitled to damages as a result of Defendants' wrongful conduct;

i) Whether Plaintiffs and the Class members are entitled to restitution as a result of Defendants' wrongful conduct;

j) What equitable relief is appropriate to redress Defendants' wrongful conduct; and

k) What injunctive relief is appropriate to redress the imminent and currently ongoing harm faced by Class members.

123. **Typicality**: Plaintiffs' claims are typical of the claims of each of the Class members. Plaintiffs and the Class members sustained damages as a result of Defendants' uniform wrongful conduct during transactions with them.

124. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Class, and has retained counsel competent and experienced in complex litigation and class actions. Plaintiffs have no interests antagonistic to those of the Class, and there are no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of the members of the proposed Class, and has the financial resources to do so. Neither Plaintiffs nor her counsel have any interest adverse to those of the other members of the Class.

125. **Separateness**: This case is appropriate for certification because prosecution of separate actions would risk either inconsistent adjudications which would establish incompatible standards of conduct for the Defendants or would be dispositive of the interests of members of the proposed Class. Furthermore, the Private Information collected by Defendants still exists, and is still vulnerable to future attacks – one standard of conduct is needed to ensure the future safety of the PHI and PII collected, stored, and maintained by Defendants.

126. **Class-wide Applicability**: This case is appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Plaintiffs and proposed Class as a whole, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct towards members of the Class, and making final injunctive relief appropriate with respect to the proposed Class as a whole. Defendants' practices challenged herein apply to and affect the members of the Class uniformly, and Plaintiffs' challenge to those practices hinges on Defendants' conduct with respect to the proposed Class as a whole, not on individual facts or law applicable only to Plaintiff.

127. **Superiority**: This case is also appropriate for certification because class proceedings are superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and the members of the Class. The injuries suffered by each individual member of the Class are relatively small in comparison to the burden and expense of individual prosecution of the litigation necessitated by Defendants' conduct. Absent a class action, it would be virtually impossible for individual members of the Class to obtain effective relief from Defendants. Even

if Class members could sustain individual litigation, it would not be preferable to a class action because individual litigation would increase the delay and expense to all parties, including the Court, and would require duplicative consideration of the common legal and factual issues presented here. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court.

COUNT I

Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

128. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

129. Defendants knew, or should have known, of the risks and responsibilities inherent in collecting and storing the PII and PHI of Plaintiffs and Class members.

130. As described above, Defendants owed a duty of care to Plaintiffs and Class members whose PII and PHI had been entrusted to Defendants.

131. Defendants breached their duty to Plaintiffs and Class members by failing to secure their PII and PHI from unauthorized disclosure to third parties.

132. Defendants acted with wanton disregard for the security of Plaintiffs and Class members' PII and PHI.

133. A "special relationship" exists between Defendants and the Plaintiffs and Class members. Defendants entered into a "special relationship" with Plaintiffs and Class members because they collected and/or stored the PII and PHI of Plaintiff and the Class members.

134. But for Defendants' wrongful and negligent breach of their duty owed to Plaintiffs and the Class members, Plaintiffs and the Class members would not have been injured.

135. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendants' breach of their duty. Defendants knew or should have known

they were failing to meet their duty, and that Defendants' breach of such duties would cause Plaintiffs and Class members to experience the foreseeable harms associated with the unauthorized exposure of their PII and PHI.

136. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II

Negligence *Per Se*
(On Behalf of Plaintiffs and the Nationwide Class)

137. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

138. Pursuant to HIPAA (42 U.S.C. §1302d *et. seq*.), Defendants had a duty to implement reasonable safeguards to protect Plaintiffs and Class members' PII and PHI.

139. Defendants breached their duty to Plaintiffs and Class members under HIPAA (42 U.S.C. § 1302d *et. seq.*), by failing to implement reasonable safeguards to protect Plaintiffs and Class members' PII and PHI from unauthorized access.

140. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

141. But for Defendants' wrongful and negligent breach of their duty owed to Plaintiff and Class members, Plaintiffs and Class members would not have been injured.

142. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duty, and that Defendants' breach of that duty would cause Plaintiffs and Class members to experience the foreseeable harms associated with the unauthorized access to their PII and PHI.

143. As a direct and proximate result of Defendants' negligent conduct, Plaintiffs and Class members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III

Breach of Implied Covenant of Good Faith and Fair Dealing (On Behalf of Plaintiffs and the Nationwide Class)

144. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

145. Plaintiffs and Class members entered into valid, binding, and enforceable express or implied contracts with entities affiliated with or serviced by Defendants, as alleged above.

146. The contracts respecting which Plaintiffs and Class members were intended beneficiaries were subject to implied covenants of good faith and fair dealing that all parties would act in good faith and with reasonable efforts to perform their contractual obligations (both explicit and fairly implied) and not to impair the rights of the other parties to receive the rights, benefits, and reasonable expectations under the contracts. These included the implied covenants that Defendants would act fairly and in good faith in carrying out their contractual obligations to take reasonable measures to protect Plaintiffs' PII and PHI from unauthorized disclosure and to comply with state laws and regulations.

147. A "special relationship" exists between Defendants and the Plaintiffs and Class members. Defendants entered into a "special relationship" with Plaintiffs and Class members who sought health care services from J&J and, in doing so, entrusted Defendants, pursuant to their requirements and Privacy Notice, with their PII and PHI.

148. Despite this special relationship with Plaintiffs, Defendants did not act in good faith and with fair dealing to protect Plaintiffs and Class members' PII and PHI.

149. Plaintiffs and Class members performed all conditions, covenants, obligations, and promises owed to Defendants.

150. Defendants' failure to act in good faith in complying with the contracts denied Plaintiffs and Class members the full benefit of their bargain, and instead they received healthcare

and related services that were less valuable than what they paid for and less valuable than their reasonable expectations.

151. Accordingly, Plaintiffs and Class members have been injured as a result of Defendants' breach of the covenant of good faith and fair dealing respecting which they are express or implied beneficiaries, and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV

Breach of Duty
(On Behalf of Plaintiffs and the Nationwide Class)

152. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

153. Defendants accepted the special confidence placed in them by Plaintiffs and Class members. There was an understanding between the parties that the healthcare service provider would act for the benefit of Plaintiffs and Class members in preserving the confidentiality of their PII and PHI.

154. Defendants became the guardian of Plaintiffs and Class members' PII and PHI and accepted a fiduciary duty to act primarily for the benefit J&J customer, including Plaintiffs and the Class members, including safeguarding Plaintiffs' and the Class members' PII and PHI.

155. Defendants breached their fiduciary duty to Plaintiffs and Class members by (a) failing to protect their PII and PHI to Plaintiff and the Class; (b) by failing to timely notify Plaintiffs and the Class members of the unauthorized disclosure of the PII and PHI; and (c) by otherwise failing to safeguard Plaintiffs' and the Class members' PII and PHI.

156. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and/or Class members have suffered and/or will suffer injury, including but not limited to: (a) the compromise of their PII and PHI; and (b) the diminished value of the services they received as a result of unauthorized exposing of Plaintiffs and Class members' PII and PHI.

157. As a direct and proximate result of Defendants' breach of their fiduciary duty, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V

Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

158. Plaintiffs, on behalf of themselves and the Class, re-allege and incorporate the above allegations by reference.

159. Defendants collected and maintained responsibility for the Private Information of Plaintiffs and the Class, including, *inter alia*, name, Social Security Number, and other PHI in connection with the provision of services to Plaintiff and the Class.

160. At the time Defendants acquired the PII of Plaintiffs and the Class, there was a meeting of the minds and a mutual understanding that Defendants would safeguard the PII and not take unjustified risks when storing the PII.

161. Plaintiffs and the Class would not have entrusted their PII to Defendants had they known that Defendants would fail to adequately safeguard their PII.

162. Implicit in the agreement between Plaintiffs and Class members and the Defendants to provide PII and PHI, was the latter's obligation to: (a) use such PII and PHI for business purposes only, (b) take reasonable steps to safeguard that PII and PHI, (c) prevent unauthorized disclosures of the PII and PHI, (d) provide Plaintiffs and Class members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII and PHI, (e) reasonably safeguard and protect the PII and PHI of Plaintiffs and Class members from unauthorized disclosure or uses, and (f) retain the PII and PHI only under conditions that kept such information secure and confidential.

163. In collecting and maintaining responsibility for the maintenance and protection of

the PII and PHI of Plaintiffs, Defendants entered into solemn duties and implied contracts with Plaintiffs and the Class requiring them to protect and keep secure the PHI/PII of Plaintiff and the Class.

164. Plaintiffs and the Class fully performed their obligations with Defendants.

165. Defendants breached their duties to and implied contracts with Plaintiffs and the Class by failing to protect and keep PHI/PII of Plaintiffs and the Class.

166. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; additional time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, credit freezes, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

167. As a direct and proximate result of Defendants' breach of contract, Plaintiffs are at an increased risk of identity theft or fraud.

168. As a direct and proximate result of Defendants' breach of contract, Plaintiffs are entitled to and demand actual, consequential, and nominal damages and injunctive relief, to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the proposed Class, prays for relief and judgment against Defendants as follows:

A. certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, appointing Plaintiffs as representatives of the Class, and designating Plaintiffs' counsel as Class Counsel;

B. declaring that Defendants' conduct violates the laws referenced herein;

C. finding in favor of Plaintiffs and the Class on all counts asserted herein;

D. awarding Plaintiffs and the Class compensatory damages and actual damages, trebled, in an amount exceeding $5,000,000, to be determined by proof;

E. awarding Plaintiffs and the Class appropriate relief, including actual, nominal and statutory damages;

F. awarding Plaintiffs and the Class punitive damages;

G. awarding Plaintiffs and the Class civil penalties;

H. granting Plaintiffs and the Class declaratory and equitable relief, including restitution and disgorgement;

I. enjoining Defendants from continuing to engage in the wrongful acts and practices alleged herein;

J. awarding Plaintiffs and the Class the costs of prosecuting this action, including expert witness fees;

K. awarding Plaintiffs and the Class reasonable attorneys' fees and costs as allowable by law;

L. awarding pre-judgment and post-judgment interest; and

M. granting any other relief as this Court may deem just and proper.

Dated: November 2, 2023

Respectfully submitted,

BARRACK, RODOS & BACINE
By: /s/ *Michael A. Toomey*
MICHAEL A. TOOMEY
11 Times Square
640 8th Ave., 10th Fl.
New York, NY 10022

Telephone: (212) 688-0782
mtoomey@barrack.com

BARRACK, RODOS & BACINE
STEPHEN R. BASSER*
SAMUEL M. WARD*
600 West Broadway, Suite 900
San Diego, CA 92101
sbasser@barrack.com
sward@barrack.com
Telephone: (619) 230-0800
Facsimile: (619) 230-1874

John G. Emerson*
EMERSON FIRM, PLLC
2500 Wilcrest, Suite 300
Houston, TX 77042
Telephone: (800) 551-8649
Facsimile: (501) 286-4659

Attorneys for Plaintiffs
**pro hac vice* application to be submitted

EXHIBIT A

INTERNATIONAL BUSINESS MACHINES CORPORATION
Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

40068272003144069 6
000 0006289 00000000 0001 0002 03145 INS: 0 0

ROWDY ALLDRIDGE
1680 E 25TH ST
IDAHO FALLS ID 83404-6300

11
3145

September 29, 2023

Notice of Data Breach

Dear Rowdy Alldridge:

This notice concerns an incident involving unauthorized access to personal information contained within a database used on the Janssen CarePath platform, a patient support platform that offers savings options and other patient support resources.

International Business Machines Corporation ("IBM" or "we") is a service provider to Johnson & Johnson Health Care Systems, Inc. ("Janssen"). IBM manages the application and the third-party database that supports Janssen CarePath. We are writing to inform you of a recent incident that may have involved unauthorized access to your personal information stored in Janssen CarePath. While we have no reason to believe that your information has been misused, we want to let you know what happened and the steps we have taken in response. This letter explains what happened, our response, and steps you can take to protect your information.

What happened: Janssen recently became aware of a technical method by which unauthorized access to the database could be obtained. Janssen then immediately notified IBM, and, working with the third-party database provider, IBM promptly remediated the issue. IBM also undertook an investigation to assess whether there had been unauthorized access to the database. While IBM's investigation identified, on August 2, 2023, that there was unauthorized access to personal information in the database, the investigation was unable to determine the scope of that access. As a result, we are notifying you out of an abundance of caution.

What information was involved: The personal information involved in this incident may have included your name and one or more of the following: contact information, health insurance information, and information about medications and associated conditions that were provided to the Janssen CarePath application. Your Social Security number and financial account information were not contained in the database or affected.

What we are doing: After being informed of the issue by Janssen, IBM and the third-party database provider promptl identified and implemented steps that disabled the technical method at issue. IBM also worked with the third-party databa provider to augment security controls to reduce the chance of a similar event occurring in the future.

What you can do: We encourage you to remain vigilant by regularly reviewing your account statements and explanation benefits from your health insurer or care providers with respect to any unauthorized activity. If you identify services that did not receive or other suspicious activity, promptly report that activity to the institution that provided the report. Additi information on steps that you can take to protect against potential misuse of personal information can be found i enclosed "Additional Resources" document, which we encourage you to review.